

B D U



REC'D 28 FEB 2000

WIPO PCT

FR 00 / 332

# BREVET D'INVENTION

09/673137

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le .....

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

### PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

Martine PLANCHE

## Best Available Copy

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

#### SIEGE

26 bis, rue de Saint Petersburg  
75800 PARIS Cédex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30

**THIS PAGE BLANK (USPTO)**

**REQUÊTE EN DÉLIVRANCE**

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

DATE DE REMISE DES PIÈCES **11.02.99**  
N° D'ENREGISTREMENT NATIONAL **99 01652-**  
DÉPARTEMENT DE DÉPÔT **75**  
DATE DE DÉPÔT **11 FEV. 1999**

**2 DEMANDE** Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire  
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen  
☐ demande initiale  
☐ brevet d'invention

**Établissement du rapport de recherche**

☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

**Procédé de vérification de l'usage de clés publiques engendrées par un système embarqué.**

**3 DEMANDEUR (S)** n° SIREN **6 4 2 0 5 8 7 3 9** code APE-NAF **3 0 0 C**

Nom et prénoms (souligner le nom patronymique) ou dénomination

**BULL S.A.**

Forme juridique

**S.A.**

Nationalité (s) **Française**  
Adresse (s) complète (s)

Pays

**BULL S.A.**

**FRANCE**

**68, route de Versailles  
78434 LOUVECIENNES CEDEX**

En cas d'insuffisance de place, poursuivre sur papier libre ☐

**4 INVENTEUR (S)** Les inventeurs sont les demandeurs ☐ oui ☒ non

Si la réponse est non, fournir une désignation séparée

**5 RÉDUCTION DU TAUX DES REDEVANCES**

☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

**6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE**

pays d'origine

numéro

date de dépôt

nature de la demande

**7 DIVISIONS** antérieures à la présente demande n°

date

n°

date

**8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE**  
(nom et qualité du signataire)

**Bernard CORLU  
Mandataire -**

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI



# BREVET D'INVENTION / CERTIFICAT D'UTILITE

## DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

### DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg  
75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

FR 3775/BC

N° D'ENREGISTREMENT NATIONAL

9901652

### TITRE DE L'INVENTION :

**Procédé de vérification de l'usage de clés publiques engendrées par un système embarqué.**

### LE(S) SOUSSIGNÉ(S)

**BULL S.A.**

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

**Pinkas Denis**  
**13 Pavé des Gardes**  
**92370 CHAVILLE**  
**France**

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

**Louveciennes, le 08 Février 1999**

**Corlu Bernard (mandataire)**

PROCEDE DE VERIFICATION DE L'USAGE DE CLES PUBLIQUES  
ENGENDREES PAR UN SYSTEME EMBARQUE

5 L'invention concerne un procédé de vérification, notamment de l'usage de clés publiques engendrées par un système embarqué.

10 Afin d'assurer la sécurité de transmission des données transmises sur les réseaux informatiques, les utilisateurs de ces réseaux ont exercé une forte demande relative à des prestations de chiffrement/déchiffrement et/ou de génération/vérification de signature numérique de ces données transmises.

15 Les opérations de chiffrement/déchiffrement ont pour but de coder puis de décoder, à partir d'une convention secrète temporairement partagée entre un émetteur et un récepteur, des messages transmis afin de rendre ces derniers inintelligibles aux tiers à cette convention.

20 Les opérations de signature ont pour objet la transmission de messages spécifiques permettant de s'assurer de l'intégrité et l'origine des données transmises.

25 Pour des raisons de sécurité publique, les Pouvoirs Publics ont, dans certains états, mis en place des dispositions législatives contraignantes afin d'imposer une réglementation stricte des opérations de chiffrement/déchiffrement utilisant des algorithmes dits "forts". Toutefois, les autres opérations telles le chiffrement/déchiffrement utilisant des algorithmes dits  
30 "faibles", l'authentification, l'intégrité et la non-répudiation utilisant un calcul de signature numérique ne font pas l'objet de telles mesures contraignantes. En particulier, le message d'information accompagnant une

signature numérique étant transmis en clair peut faire l'objet de tout contrôle de police utile.

Différents systèmes de calcul de signatures numériques ont, jusqu'à ce jour, été proposés.

5        Parmi ceux-ci, les systèmes cryptographiques à clés asymétriques ont été plus particulièrement développés en raison de leur souplesse d'utilisation ou tout au moins de la souplesse relative de gestion des clés précitées. En effet, ces systèmes mettent en œuvre une clé privée, non  
10        publiée, et une clé publique. La connaissance de la clé publique ne permet pas de calculer la clé privée.

       Certains algorithmes de signature numérique ne peuvent servir à un autre usage que la signature numérique. C'est ainsi le cas du système connu sous le nom de DSA  
15        (Digital Signature Algorithm). Cependant il existe un autre algorithme largement utilisé connu sous le nom de RSA, du nom de leurs inventeurs RIVEST, SHAMIR et ADLEMAN, lequel permet à la fois la mise en œuvre d'opérations de calcul de signature numérique et de chiffrement/déchiffre-  
20        ment, dit "fort".

       La présente invention a, en autres objets, dans le cadre de la mise en œuvre d'un système cryptographique à clés asymétriques, de s'assurer qu'un système embarqué utilisant l'algorithme RSA et des clés RSA à usage de  
25        signature seulement sera en mesure de supporter uniquement des opérations de signature à partir de cesdites clés et en aucun cas des opérations de déchiffrement.

       Un autre objet de la présente invention est la mise en place d'une infrastructure de clés publiques utilisable  
30        exclusivement à des fins de signature numérique. En effet, si un utilisateur tentait d'utiliser à des fins de chiffrement l'une des clés publiques RSA ainsi certifiées à des fins de signature, l'entité en possession de la clé

privée RSA correspondante se trouverait dans la totale incapacité de pouvoir déchiffrer en utilisant ladite clé privée.

5 Un autre objet de la présente invention est également un procédé de vérification d'une requête de certification de clé publique engendrée par un système embarqué permettant un contrôle, par une autorité de certification, de l'usage de cette clé à des fins d'opérations de déchiffrement limitées.

10 Un autre objet de la présente invention est enfin, dans le cadre du contrôle précité de l'usage de cette clé, la limitation de cet usage à des opérations de chiffrement/déchiffrement au moyen d'algorithmes symétriques "faibles" autorisés par certains pouvoirs publics.

15 On rappelle que les systèmes embarqués sont, de manière générale, constitués par une carte à microprocesseur et mis à la disposition d'une entité.

20 La notion d'entité précitée recouvre soit la personne physique titulaire d'un système embarqué telle qu'une carte à microprocesseur, soit tout système informatique muni d'un système embarqué ou carte à microprocesseur comparable.

25 Le procédé de vérification de l'origine de la requête de certification d'une clé publique issue d'un jeu de clés asymétriques, clé publique  $K_p$  et clé privée  $K_s$  engendrées, pour un algorithme donné CA1 et pour un usage donné, tel que le chiffrement/déchiffrement ou la vérification/ génération de signature numérique, par un système embarqué et mémorisées dans la zone mémoire d'un

30 système embarqué Si muni de moyens de calcul cryptographique et de moyens de mémorisation de données numériques à accès externe protégé en écriture/lecture, ces

données numériques  $IDd_i$  comportant au moins un numéro de série  $SN_i$  permettant l'identification du système embarqué et un code d'identification  $OP_i$  d'un opérateur habilité à configurer ledit système embarqué et cette requête étant formulée par ledit système embarqué par transmission d'un message de requête MRCA contenant ladite clé publique  $Kp$  à une autorité de certification CA est remarquable en ce qu'il consiste, préalablement à toute transmission d'une requête de certification, lors de la configuration de ces systèmes embarqués par cet opérateur habilité, pour tous les systèmes embarqués  $Si$  d'un ensemble  $Lk$  de systèmes embarqués :

- à faire engendrer par cet opérateur habilité, pour cet ensemble donné de systèmes embarqués, une clé publique mère  $KpM$  et une clé privée mère  $KsM$  ;

- à publier ladite clé publique mère  $KpM$  associée d'une part à l'identité de cet opérateur habilité  $OP_i$  et d'autre part à cet ensemble  $Lk$  de systèmes embarqués ; et pour chaque système embarqué appartenant à la plage d'identifiants définie par l'ensemble  $Lk$  de systèmes embarqués :

- à faire engendrer par cet opérateur habilité, à partir de ladite clé privée mère  $KsM$  et du numéro de série  $SN_i$  du système embarqué, une clé privée diversifiée  $KsM_i$  et à mémoriser, dans ladite zone mémoire à accès externe protégé en écriture/lecture, ladite clé privée diversifiée  $KsM_i$ , et préalablement à toute transmission d'une requête de certification,

- à faire engendrer par l'intermédiaire du système embarqué une requête de certification RCA, contenant en particulier un champ de clé publique  $CAI, Kp$  et les indicateurs d'usage  $U$  de cette clé publique;



- à faire engendrer par l'intermédiaire du système embarqué, au moyen desdits moyens de calcul et de ladite clé diversifiée  $KsM_1$ , associée à ce système embarqué, une valeur de contrôle cryptographique  $Sc_1$  sur l'ensemble de la requête RCA, cette valeur de contrôle cryptographique étant  
 5 une signature numérique calculée au moyen de la clé privée diversifiée  $KsM_1$  ; et lors de l'émission, par le système embarqué, d'une requête de certification à l'autorité de certification :

10 - à former un message de requête de certification MRCA contenant la requête RCA, l'identifiant  $IDd_1$  du système embarqué, ce dernier étant constitué d'une part de l'identifiant  $OP_j$  de cet opérateur habilité et d'autre part du numéro de série  $SN_1$  du système embarqué, et la valeur de  
 15 contrôle cryptographique  $Sc_1$ ,

- à transmettre à l'autorité de certification CA ledit message de requête MRCA formé lors de l'étape précédente et contenant les champs de clé publique  $CA_1, Kp$  et les indicateurs d'usage  $U$ , objets de ladite  
 20 certification, et ladite valeur de contrôle cryptographique  $Sc_1$  ;

- à retrouver, lors de la réception d'un message de requête de certification MRCA par l'autorité de certification, l'identité de l'opérateur habilité  $OP_j$  à partir de l'identifiant  $IDd_1$  du système embarqué,  
 25

- à retrouver, à partir de l'identifiant  $OP_j$  de l'opérateur habilité, la valeur de la clé publique mère  $KpM$  associée à l'ensemble  $Lk$  auquel appartient le système embarqué ;

30 - à vérifier, à partir de ladite clé publique mère  $KpM$ , dudit numéro de série  $SN_1$  du système embarqué, dudit message de requête de certification reçue MRCA, ladite valeur de contrôle cryptographique  $Sc_1$ , ce qui permet

d'établir l'authenticité de cette valeur de contrôle cryptographique et de l'origine de cette requête de certification.

Le procédé de vérification d'une requête de certification de clé engendrée par un système embarqué, objet de l'invention, s'applique à tout type de système embarqué, mais plus particulièrement à des systèmes embarqués en nombre constitués chacun par une carte à microprocesseur ou analogue.

Il sera mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels, outre la figure 1 relative à un système embarqué, constitué par une carte à microprocesseur de type classique,

- la figure 2a représente, à titre d'exemple non limitatif, un organigramme de l'ensemble des opérations ou étapes permettant la mise en œuvre du procédé objet de la présente invention, c'est à dire de la génération d'une requête de certification générée par le système embarqué;

- la figure 2b représente, à titre d'exemple non limitatif, un organigramme d'une variante de mise en œuvre du procédé, objet de la présente invention, tel que représenté en figure 2a et dans lequel un contrôle de la syntaxe d'un gabarit de requête de certification fournie au système embarqué est effectué par le système embarqué, préalablement à la génération de ladite requête de certification ;

- la figure 3 représente, sous forme d'un diagramme fonctionnel, le détail de l'étape du procédé mis en œuvre ainsi qu'illustré en figure 2a ou 2b, dans laquelle une clé privée diversifiée est calculée pour chaque système embarqué ;

- la figure 4a représente, à titre d'exemple non limitatif, la structure d'un message de requête de certification dans une version simplifiée, permettant la mise en œuvre du procédé objet de l'invention tel que représenté en figure 2a ;

- la figure 4b représente, à titre d'exemple non limitatif, la structure d'un message de requête de certification dans une version améliorée et codé au format ASN1 selon une structure TLV, plus particulièrement destinée à la mise en œuvre du procédé objet de l'invention tel que représenté en figure 2b ;

- la figure 5 représente, sous forme d'un diagramme fonctionnel, le détail de l'étape du procédé mis en œuvre ainsi qu'illustré en figure 2a ou 2b, dans laquelle une vérification du message de requête est effectuée par l'autorité de certification ;

- la figure 6 représente une variante particulièrement avantageuse de mise en œuvre du procédé objet de la présente invention, dans laquelle à la clé privée associée à une clé publique, objet d'une requête de certification, est associée une clé symétrique de chiffrement/déchiffrement faible, au système embarqué correspondant étant ainsi conféré une fonction de chiffrement/déchiffrement faible, satisfaisant aux dispositions légales en vigueur dans certains pays en vue d'une commercialisation de ces systèmes en l'absence d'une autorisation préalable.

Une description plus détaillée du procédé de vérification de la requête de certification d'une clé publique conforme à l'objet de la présente invention sera maintenant donnée en liaison avec les figures 2a, 2b et les figures suivantes.

Préalablement à la description détaillée des étapes nécessaires à la mise en œuvre du procédé en liaison avec les figures précitées, des considérations d'ordre général visant à illustrer le contexte de mise en œuvre du procédé, objet de la présente invention, seront données ci-après.

5 D'une manière générale, le procédé objet de la présente invention permet d'assurer la vérification d'une requête de certification de clé publique engendrée par un système embarqué, cette vérification comportant notamment la vérification de l'origine de cette requête, mais  
10 également compte tenu de la vérification ainsi effectuée et de la certitude ainsi obtenue de l'origine de cette requête, d'avoir la certitude que la clé privée correspondant à la clé publique générée faisant l'objet de la présente requête de certification ne pourra servir qu'à  
15 des usages bien spécifiés, telle la génération de signature numérique ou le déchiffrement de clés symétriques faibles.

Les clés publiques étant, comme leur nom l'indique, publiques, il ne saurait être question de pouvoir limiter  
20 l'usage de ces clés pour le chiffrement. Cependant les clés privées étant nécessairement protégées, le mécanisme de protection mis en œuvre pourra être en mesure d'empêcher l'usage de clés privées RSA à des fins de déchiffrement. Si donc l'opération de chiffrement ne peut être interdite,  
25 l'opération de déchiffrement peut l'être et donc le processus de chiffrement/déchiffrement devient ainsi impossible. La procédure mise en œuvre s'appuie sur le fait qu'il est possible de s'assurer que la clé privée correspondant à une clé publique donnée ne pourra être  
30 utilisée à des fins de déchiffrement de par le fait qu'il est possible d'être sûr qu'elle est effectivement contenue dans un système embarqué protégé empêchant son usage à des fins de déchiffrement.

Afin de s'assurer qu'une clé donnée est attachée à une entité donnée, une technique de certification des clés est actuellement largement utilisée. Cette technique consiste à faire engendrer par une Autorité de Certification AC un certificat de clé publique qui associe à un nom d'entité donné, un identifiant d'algorithme à clé publique CA1, une valeur de clé publique Kp, pour des usages donnés U et ce, pour une période de validité donnée. Un exemple de tel certificat est connu sous le nom de certificat X.509 du nom de la norme de l'ITU (International Telecommunications Union) qui l'a normalisé.

Afin de pouvoir participer à une architecture supportant des clés publiques il est nécessaire de pouvoir disposer d'un certificat de clé publique. Pour cela il est nécessaire de formuler une requête qui comporte les informations que le demandeur souhaite voir figurer dans son certificat. Cette requête comporte en particulier l'identifiant de l'algorithme utilisé CA1, la valeur de la clé publique Kp pour cet algorithme et les usages de cette clé U. Si la requête émane directement de l'entité il est impossible de connaître les protections mises en œuvre pour la clé privée correspondante. Cependant si la requête émane directement d'un système embarqué protégé empêchant l'usage de la clé privée à des fins de déchiffrement, alors il est possible de s'assurer que la clé privée correspondant à la clé publique qui fait l'objet de la demande de certification ne pourra être utilisable que pour les usages indiqués, par exemple à des fins de génération de signature ou de déchiffrement de clés faibles. C'est l'un des objets du procédé objet de la présente invention, lequel sera décrit ci-après en détail en liaison avec les figures 2a et 2b.

Le procédé, objet de la présente invention, sera décrit maintenant dans le cas non limitatif où le système embarqué est constitué par une carte à microprocesseur telle qu'une carte bancaire, une carte PCMCIA analogue.

5 De manière classique, ainsi que représenté sur la figure 1, une carte à microprocesseur 10 comprend un système d'entrée/sortie 12, reliée au microprocesseur 14, une mémoire RAM 16, une mémoire non volatile 18, constituée par une mémoire morte ROM 18b et une mémoire programmable 18a. L'ensemble de ces éléments est relié au microprocesseur 14 par une liaison par BUS. Un module 20 de calcul cryptographique de données est, en outre, ajouté. La mémoire non volatile 18 comporte habituellement une zone mémoire à accès protégé en écriture/lecture, notée MAP, 15 l'accès de cette zone étant réservé au seul microprocesseur 14 à des fins d'utilisation purement interne.

En référence à la figure 1, on indique que dans une telle carte à microprocesseur, le module de calcul cryptographique peut contenir des programmes de génération ou vérification de signature, de chiffrement/déchiffrement 20 mis en œuvre à partir de processus dits "forts" supportés par l'algorithme RSA par exemple, ainsi que des processus dits "faibles" supportés par des algorithmes tel que le DES limité à des tailles de clé de 40 bits par exemple.

25 Conformément à la figure 2a, un opérateur habilité, identifié par un identifiant  $OP_i$ , est en situation à l'étape 1000 de procéder à une configuration d'un ensemble de systèmes embarqués, cet ensemble étant noté Lk. D'une manière pratique, on indique que cet ensemble correspond à un lot de systèmes embarqués tel que des cartes à 30 microprocesseur par exemple, que cet opérateur souhaite distribuer dans le commerce. Cet opérateur habilité peut bien entendu être soit le fabricant de cartes à mémoire

soit tout sous-traitant habilité par ce dernier ou par une autorité publique ou privée agréée. Chaque système embarqué est en outre doté d'un numéro d'identification noté  $SN_i$  et, dans le cadre de la mise en œuvre du procédé, objet de la présente invention, chaque système embarqué  $S_i$  appartenant à l'ensemble  $L_k$  donné est donc muni d'un numéro d'identification, noté  $IDd_i$ , constitué par l'identifiant de l'opérateur habilité  $OP_j$  et par le numéro de série  $SN_i$  de ce système embarqué.

Afin de vérifier notamment l'origine de la requête de certification d'une clé publique issue d'un jeu de clés asymétriques, clé publique  $K_p$  et clé privée  $K_s$ , engendrées par un système embarqué appartenant à l'ensemble de systèmes embarqués précité, ces clés publique  $K_p$  et privée  $K_s$  étant engendrées pour un usage donné tel que le chiffrement/déchiffrement ou la vérification/génération de signature numérique par exemple, le procédé objet de la présente invention consiste, préalablement à toute transmission d'une requête de certification, lors d'une étape de configuration des systèmes embarqués par l'opérateur habilité à réaliser cette configuration, à faire engendrer, en une étape 1001, par cet opérateur habilité et pour l'ensemble de systèmes embarqués, une clé publique mère, notée  $K_{pM}$ , et une clé privée mère  $K_{sM}$  destinées à être mises en œuvre dans le cadre d'un processus supporté par l'algorithme CalM relatif aux clés  $K_{pM}$  et  $K_{sM}$ .

L'étape 1001 précitée, suivie d'une étape 1002 consistant à publier la clé publique mère  $K_{pM}$  associée d'une part à l'identité de l'opérateur habilité  $OP_j$  et d'autre part à l'ensemble  $L_k$  de systèmes embarqués. Ainsi que représenté à l'étape 1002 sur la figure 2a, cette publication peut consister en une publication de quatre

valeurs liées sous forme d'une liste par exemple, c'est-à-dire de l'identifiant de l'opérateur habilité  $OP_j$ , d'une plage d'identifiants définie par l'ensemble  $L_k$  et bien entendu de la valeur de la clé publique mère  $KpM$  associée au code indicateur de l'algorithme à mettre en œuvre  $CALM$ . La plage d'identifiants peut être constituée par un identifiant de début et de fin de plage.

Lors de cette étape de configuration par l'opérateur habilité, on indique que la création des clés, clé publique mère  $KpM$  et clé privée mère  $KsM$ , est directement dépendante de l'algorithme utilisé et ne peut donc être décrite de manière indépendante du processus supporté par l'algorithme mis en œuvre. Le type d'algorithme à mettre en œuvre est cependant précisé ci-après.

A la suite de l'étape 1002 précitée, le procédé, objet de la présente invention consiste, pour chaque système embarqué  $S_i$  appartenant à l'ensemble  $L_k$  des systèmes embarqués, à calculer en une étape 1003, à partir de la clé privée mère  $KsM$  et du numéro de série  $SN_i$  de chaque système embarqué considéré  $S_i$ , une clé privée diversifiée, notée  $KsM_i$ .

Conformément à un aspect particulièrement avantageux du procédé, objet de la présente invention, la clé privée diversifiée  $KsM_i$  est alors mémorisée dans la zone mémoire à accès externe protégé en lecture/écriture MAP de la carte à microprocesseur constituant le système embarqué.

D'une manière générale, on indique que la clé privée diversifiée  $KsM_i$  est unique et distincte pour chaque système embarqué dont l'identifiant  $SN_i$  est différent dans l'ensemble  $L_k$ .



Suite à l'étape 1003 précédemment mentionnée, le procédé, objet de la présente invention, consiste, dans une version avantageuse, préalablement à toute transmission d'une requête de certification et pour toute clé publique Kp à certifier à la demande de chaque système embarqué Si  
5 considéré, cette demande étant bien entendu formulée par un utilisateur Uti, c'est-à-dire par une entité, à faire engendrer, en une étape 1004-5, par l'intermédiaire du système embarqué, une requête de certification RCA  
10 contenant en particulier un champ de clé publique CA1, Kp et les indicateurs d'usage U de cette clé publique. Lorsque la requête de certification RCA est engendrée directement par le système embarqué, le procédé peut consister à engendrer, au niveau du système embarqué, la requête de certification  
15 RCA. Celle-ci est alors composée de trois champs, soit un identifiant d'algorithme à clé publique CA1, une valeur de clé publique Kp et un indicateur des usages de cette clé U.

Dans un mode de réalisation spécifique non limitatif, l'étape 1004-5 peut par exemple consister à  
20 communiquer, en une étape 1004, au système embarqué d'identifiant SN<sub>i</sub> considéré, un gabarit de requête de certification, noté GRCA, ce gabarit contenant tous les champs requis hormis les champs de clé publique de déchiffrement ou de vérification de signature numérique  
25 ainsi que les indicateurs d'usage U de la clé publique Kp, objets de la certification demandée.

La vérification du gabarit de requête de certification GRCA sera décrite de manière plus détaillée ultérieurement dans la description.

30 Le gabarit de requête de certification GRCA permet alors, en une étape 1005, au système embarqué considéré, d'effectuer une opération consistant à compléter les champs manquants du gabarit de requête de certification GRCA.

Ainsi, le champ de clé publique, champ comportant l'identifiant d'un algorithme CA1 de chiffrement/déchiffrement ou de calcul de signature, par exemple l'algorithme RSA précité, et une valeur de clé publique  $K_p$ , objet de la certification demandée, ainsi que le champ relatif aux indicateurs d'usage U de cette clé publique sont complétés afin de reconstituer une requête de certification complète, notée RCA, à l'étape 1005 suivante.

Sur la figure 2a, on a représenté l'étape 1005 comme consistant à faire effectuer le complément par le système embarqué des champs manquants précités, le symbole + représentant cette opération de complément. D'une manière générale, on indique que l'opération de complément précitée peut consister soit à attribuer des valeurs adéquates à des valeurs fictives déjà présentes dans le gabarit de requête de certification GRCA dans des champs déterminés, soit le cas échéant à compléter ce gabarit de requête par des opérations de concaténation au moyen de ces valeurs adéquates ainsi qu'il sera décrit ultérieurement dans la description.

L'étape 1004-5 ou l'étape 1005 précitée est alors suivie d'une étape 1006 consistant à calculer, grâce à la mise en œuvre du module de calcul du système embarqué considéré et de la clé diversifiée  $K_{SM_i}$  associée à ce système embarqué à l'étape 1003, une valeur de contrôle cryptographique, notée  $SC_i$ .

D'une manière générale, on indique que la valeur de contrôle cryptographique précitée est calculée sur l'ensemble de la requête complétée RCA ainsi que sur l'identifiant  $ID_{d_i}$  du système embarqué considéré. On rappelle que l'identifiant  $ID_{d_i}$  du système embarqué Si est constitué par l'identifiant  $Op_i$  de l'opérateur habilité et par le numéro de série  $SN_i$  du système embarqué.

De préférence, la valeur de contrôle cryptographique  $SC_i$  est une signature numérique calculée au moyen de la clé privée diversifiée  $KSM_i$ .

Pour cette raison la valeur de contrôle cryptographique vérifie la relation :

$$SC_i = S_{KSM_i}(RCA, IDd_i)$$

Dans cette relation, on indique que l'indice  $KSM_i$  affecté à l'opération de signature  $S$  indique le calcul de cette signature à partir de la clé privée diversifiée  $KSM_i$  sur les arguments  $RCA$  et  $IDd_i$ .

Le procédé, objet de la présente invention, consiste alors, lors de l'émission par le système embarqué considéré d'une requête de certification à l'autorité de certification, cette opération étant notée "Requête par  $Ut_i$ " sur la figure 2a, à former, à l'extérieur du système embarqué, en une étape 1007, un message de requête de certification, noté  $MRCA$ , composé de la requête complétée  $RCA$  par le système embarqué considéré, de l'identifiant du système embarqué, ainsi que de la valeur de contrôle cryptographique  $SC_i$  considérée.

Suite à l'étape 1007 précitée, une étape 1008 est prévue, laquelle consiste à transmettre à l'autorité de certification  $CA$  le message de requête  $MRCA$  formé lors de l'étape 1007 précédente. Le message  $MRCA$  contient en particulier la requête de certification complétée de la clé publique  $Kp$  dont la certification est demandée ainsi que de ses indicateurs d'usage  $U$ , cette clé publique  $Kp$  et ces indicateurs d'usage étant ainsi l'objet de la certification demandée précitée.

Le procédé, objet de la présente invention, consiste ensuite, lors de la réception d'un message de requête de certification  $MRCA$  précité, pour l'autorité de certification, à effectuer les opérations consistant à

l'étape 1009 à retrouver l'identité de l'opérateur habilité  $OP_j$ , ainsi que l'identifiant  $SN_i$  du système embarqué à partir de l'identifiant  $IDD_i$  du système embarqué, puis, à l'étape 1010, à retrouver, la plage d'identifiants  $Lk$  à laquelle appartient l'identifiant  $SN_i$  à partir des données publiées par l'opérateur  $Op_j$ , puis, à l'étape 1011 à retrouver à partir des données de l'ensemble  $Lk$ , l'identifiant du processus supporté par l'algorithme à mettre en œuvre CALM, la valeur de la clé publique mère  $KpM$  associée à l'ensemble  $Lk$ .

On comprend en particulier qu'aux étapes 1009, 1010 et 1011, la publication à l'étape 1002 des variables liées  $OP_j$  identifiant de l'opérateur habilité,  $Lk$  identifiant de l'ensemble considéré, CALM identifiant l'algorithme à mettre en œuvre, et  $KpM$  valeur de la clé publique mère associée à cet ensemble de systèmes embarqués, permette de retrouver successivement l'identifiant de cet opérateur habilité puis la valeur de la clé publique  $KpM$  ainsi que l'identifiant de l'algorithme à mettre en œuvre CALM par exemple à partir des quatre variables liées publiées.

Suite à l'obtention par l'autorité de certification de la valeur de la clé publique mère  $KpM$  précitée, une étape 1012 est alors réalisée, laquelle consiste à vérifier, à partir de la valeur de la clé publique mère  $KpM$ , du numéro de série  $SN_i$  du système embarqué et de la requête de certification complète reçue RCA, la valeur de contrôle cryptographique  $Sc_i$ . L'opération de vérification de la valeur de contrôle cryptographique  $Sc_i$  vérifie la relation :

On indique que cette opération de vérification consiste en une opération de vérification de signature, opération duale de l'opération de signature réalisée à l'étape 1006 pour

obtenir la valeur de contrôle cryptographique  $Sc_1$ . Ainsi, à l'étape 1012, l'opération de vérification de signature est réalisée à partir de la clé publique mère  $KpM$ .

5 La mise en œuvre du procédé, objet de la présente invention, tel que décrit en liaison avec la figure 2a permet ainsi d'établir l'authenticité de la valeur de contrôle cryptographique précitée et en conséquence, notamment, l'origine de la requête de certification présentée à l'autorité de certification.

10 Dans des conditions qui seront explicitées ultérieurement dans la description, la vérification de cette requête, l'origine étant établie, permet, à partir de la valeur d'usage  $U$  précitée, de connaître de manière certaine le ou les usages dédiés qui peuvent être effectués  
15 avec la clé publique  $Kp$ , du fait des usages restrictifs sur les opérations pouvant être réalisés à l'aide de la clé privée  $Ks$  contenue dans le système embarqué. On peut alors émettre un certificat à même de garantir l'usage qui peut être fait de cette clé publique du fait des restrictions  
20 sur les opérations pouvant être réalisés à l'aide de la clé privée correspondante. Cette garantie d'usage pourra provenir de l'emploi combiné de deux informations qui seront alors présentes dans le certificat généré : d'une part l'indicateur d'usage de la clé publique et d'autre  
25 part un identifiant de politique de sécurité. Cette politique de sécurité pourra alors indiquer que la génération de clé a été faite sur un système embarqué réunissant les qualités requises pour limiter l'usage des clés privées générées sur ce système embarqué. On pourra  
30 aussi utiliser toute autre champ d'extension du certificat tel que cela est explicitement prévu par le standard X.509 v3.

Une variante de mise en œuvre du procédé, objet de la présente invention et permettant la vérification d'un gabarit de requête de certification GRCA, tel que décrit en figure 2a, sera maintenant donnée en relation avec la figure 2b. Dans les figures 2a et 2b, les mêmes étapes portent les mêmes références.

Ainsi qu'on pourra l'observer sur la figure 2b, suite à l'étape 1004 consistant à communiquer au système embarqué Si un gabarit de requête de certification GRCA mais préalablement à l'étape 1005 consistant à faire compléter par le système embarqué Si les champs manquants du gabarit de requête de certification GRCA, le procédé, objet de la présente invention, peut consister en outre à vérifier, en une étape 1004a, au niveau du système embarqué Si considéré, la syntaxe du gabarit de requête de certification précité afin de s'assurer qu'il s'agit bien d'une requête de certification. L'étape 1004a peut alors être suivie d'une étape 1004b consistant par exemple en une étape de test de la valeur vraie de cette vérification de syntaxe. A l'étape 1004a, la vérification de syntaxe est notée  $V(\text{GRCA})$  et l'étape de test 1004b est notée  $V(\text{GRCA})=\text{vraie}$ .

L'étape 1005 consistant à faire compléter par le système embarqué Si les champs manquants du gabarit de requête de certification GRCA peut alors être conditionnée à une vérification positive, c'est-à-dire à une réponse positive à l'étape de test 1004b précédemment mentionnée.

Au contraire, sur réponse négative à l'étape 1004b précitée, un retour 1004c à l'étape de chargement du gabarit de requête de certification GRCA à l'étape 1004 peut alors être prévu.

L'étape de vérification de syntaxe peut être conduite par une vérification de la syntaxe du gabarit de

requête de certification GRCA, le processus de vérification précité pouvant dépendre de la structure du gabarit de requête de certification utilisée. Un exemple de processus de vérification de syntaxe sera donné ultérieurement dans la description.

5           Ainsi, le procédé objet de la présente invention permet, selon un premier aspect, de donner l'usage de la clé privée  $K_s$  à l'entité et en aucun cas de donner la connaissance de la valeur de cette clé privée à cette entité. Afin d'empêcher la connaissance de la valeur de la  
10           clé privée, le couple clé privée/clé publique est engendré par le système embarqué protégé et la clé privée est mise en œuvre par un algorithme situé directement dans le système embarqué. En aucun cas elle ne peut donc être  
15           connue à l'extérieur du système embarqué.

          Selon un deuxième aspect remarquable du procédé objet de l'invention, afin de vérifier que la demande de certification d'une clé publique émane bien du système embarqué le procédé met en œuvre plusieurs techniques. En  
20           particulier il met en œuvre le calcul d'une somme de contrôle cryptographique qui permet de s'assurer que la requête émane bien d'un système embarqué personnalisé par l'opérateur OPj. L'état de l'art met déjà en œuvre  
25           certaines de ces techniques qui s'avèrent être peu souples d'emploi, comme il va être rappelé ci-dessous. Une première technique consiste à mettre dans chaque système embarqué une clé secrète à partir de laquelle sera effectué le calcul de la somme de contrôle cryptographique. L'inconvénient majeur de cette technique connue est de  
30           devoir communiquer à l'avance à chaque autorité de certification potentielle, et de manière confidentielle, la valeur secrète de chaque système embarqué. Une première amélioration du dispositif consiste à utiliser un secret

mère et à calculer le secret de chaque système embarqué à partir à la fois du numéro de série du système embarqué et du secret mère. L'inconvénient majeur, dans ce dernier cas, est de devoir communiquer à l'avance à chaque autorité de certification potentielle et de manière confidentielle la valeur secrète de chaque secret mère correspondant à un ensemble donné de systèmes embarqués.

Une originalité de l'invention est au contraire de ne communiquer au préalable aucune information confidentielle mais de rendre accessible à chaque autorité de certification potentielle que des informations publiques, à savoir: un identifiant d'opérateur habilité  $OP_i$ , une référence de l'ensemble  $L_k$  et bien entendu une valeur de la clé publique mère  $K_{PM}$  associée à un indicateur de l'algorithme à mettre en œuvre CALM.

Ces informations permettent alors à n'importe quelle autorité de certification de vérifier l'origine de la requête de n'importe quel système embarqué faisant partie d'un ensemble de systèmes embarqués.

Une description plus détaillée de la mise en œuvre de l'étape 1003 de calcul de chaque clé privée diversifiée  $K_{SM_i}$  sera maintenant donnée en liaison avec la figure 3, le mode opératoire du calcul précité pouvant être mis en œuvre quel que soit le mode de réalisation du procédé, objet de l'invention, tel que décrit précédemment en liaison avec la figure 2a ou la figure 2b.

Le processus de diversification des clés mis en œuvre à l'étape 1003 tel que représenté en figure 3 peut ainsi consister en un processus supporté par un algorithme mis en œuvre sous le nom de Mécanisme de Signature à Apport Nul de Connaissance (*zero knowledge* en anglais) et des algorithmes connus sous le nom de FIAT-SHAMIR ou GUILLOU-QUISQUATER utilisables à cette fin. Pour cette raison,



ainsi qu'indiqué en figure 3, chaque clé privée diversifiée  $K_{SM_i}$  est réputée obtenue par la mise en œuvre de processus supportés par les algorithmes de FIAT-SHAMIR F-S ou de GUILLOU-QUISQUATER G-Q et vérifie ainsi la relation :

$$K_{SM_i} = D-F-S(K_{SM}, SN_i)$$

$$K_{SM_i} = D-G-Q(K_{SM}, SN_i)$$

relation dans laquelle D-F-S et D-G-Q désignent la mise en œuvre des processus de diversification de clé supportés par les algorithmes de FIAT-SHAMIR et de GUILLOU-QUISQUATER respectivement.

La technique utilisée consiste à mettre dans chaque système embarqué une clé privée diversifiée calculée à partir du numéro de série du système embarqué et d'une clé privée mère, laquelle clé diversifiée servira au calcul de la somme de contrôle cryptographique. L'Autorité de Certification CA sera alors en mesure de vérifier l'exactitude de la somme de contrôle cryptographique ainsi calculée en mettant en œuvre l'algorithme CALM correspondant au type d'algorithme utilisé et en utilisant uniquement le numéro de série du système embarqué et la clé publique mère correspondant à l'ensemble  $L_k$  dont fait partie le système embarqué.

De ce fait il n'est pas utile de connaître à l'avance quelle Autorité de Certification sera choisie par l'entité car chaque Autorité de Certification sera en mesure, et en particulier postérieurement à la réception de la requête de certificat, d'obtenir la clé publique mère correspondant à l'ensemble dont le système embarqué fait partie. La gestion d'un nombre important de systèmes embarqués, par exemple plusieurs millions, se trouve ainsi grandement simplifiée, permettant ainsi une large diffusion de tels systèmes cryptographiques, en stricte conformité

avec les dispositions législatives nationales en autorisant l'utilisation.

Différents éléments descriptifs de la structure de messages ou de données utilisés pour la mise en œuvre du procédé, objet de la présente invention, seront maintenant donnés en liaison avec les figures 4a à 4c.

Sur la figure 4a, on a représenté la structure d'un message de requête de certification dans une version simplifiée. Dans ce mode de réalisation simplifié, le système embarqué génère seul l'ensemble des champs de la requête RCA en concaténant les informations suivantes: le champ de clé publique qui comprend l'identifiant de l'algorithme utilisé CA1, la valeur de la clé publique Kp, et un champ d'usage de clé U, objets de la certification demandée. Ces champs peuvent, par exemple, faire l'objet d'un codage conforme au standard ASN1, pour *Abstract Syntax Notation 1* en vocable anglo-saxon, afin de pouvoir délimiter la taille de chaque champ et d'être sûr de la nature de chaque champ. Enfin, la valeur cryptographique de contrôle SC<sub>i</sub>, est calculée sur les informations précédentes puis ajoutée aux informations précédentes.

Dans ce mode de réalisation simplifié, l'ensemble des champs précité permet la mise en œuvre du procédé, objet de la présente invention, tel que représenté en figure 2a par exemple.

La figure 4b représente une structure de messages de requête complétée par exemple, au format conforme au codage ANS1 précité. Dans ce cas, le codage de ces messages est effectué selon le mode dit TLV où T désigne le type du champ, L la longueur de celui-ci et V la valeur du champ.

Sur la figure 4b, au point 1), on a représenté dans un tel cas la structure d'un gabarit de requête de certification GRCA, lequel est réputé formé par une suite

de champs TLV séquentiels ou imbriqués conformes au standard ASN1. Ce gabarit de requête est formé à l'extérieur du système embarqué. Il devra comporter, et cela est vérifié par le système embarqué, trois champs et  
 5 seulement trois champs correspondant à : 1) un type de champ d'identifiant d'algorithme, 2) un type de champ de valeur de clé publique, 3) un type de champ d'un indicateur des usages de clé publique. L'emplacement de chacun de ces champs parmi les autres champs du gabarit de requête doit  
 10 en outre correspondre à un emplacement bien précis, c'est à dire être précédé et suivi de différents types de champs prédéterminés.

Dans ces conditions, à partir du gabarit de requête de certification GRCA précité, la vérification de syntaxe  
 15 représentée à l'étape 1004b de la figure 2b peut consister, à vérifier la valeur du type du premier champ, puis en fonction de ce type ou de la longueur de ce champ de passer au type suivant. Au passage il convient de mémoriser l'ensemble des divers types rencontrés puis de vérifier que  
 20 les trois types de champs attendus sont situés aux endroits où ils doivent être placés. Pour chacun des trois champs, il convient ensuite de vérifier leur longueur et pour le champ CA1 sa valeur. En effet, il s'agit de vérifier que le type d'algorithme attendu correspond bien au type de clé  
 25 généré et correspondant à cet algorithme. Pour les champs formés à l'extérieur du système embarqué qui devront contenir en définitive la valeur de la clé publique Kp et la valeur des indicateurs d'usage de la clé U ces derniers peuvent contenir n'importe quelle valeur, les valeurs 0 ou  
 30 1 telles que représentées en figure 4b, puisque le système embarqué va leur substituer les valeurs adéquates et générées en interne

Suite à la reconnaissance à la valeur vraie de la vérification ainsi effectuée, vérification notée V(GRCA) de l'étape 1004a de la figure 2b, les valeurs des deux champs peuvent être substituées par les valeurs générées par le système embarqué. Le champ d'usage U substitué peut  
 5 consister en une chaîne de bits, le premier bit représentant par exemple un usage de chiffrement/déchiffrement C/D, la valeur 1 indiquant le chiffrement et la valeur 0 l'absence de chiffrement, le  
 10 deuxième bit correspondant par exemple à un usage de signature numérique ou d'authentification A, le troisième bit correspondant par exemple à une opération de non-répudiation NR mettant en œuvre une signature numérique par exemple.

15 En ce qui concerne la valeur de la clé publique Kp, celle-ci peut être substituée à partir des valeurs de bit de cette clé correspondante.

Enfin, en référence à la figure 4c, la structure du gabarit de requête de certification GRCA, chargée à  
 20 l'initiative de l'utilisateur Uti, peut comporter un champ relatif à un identifiant de cet utilisateur Uti, un champ relatif à la valeur de la clé Kp, clé publique dont la certification est demandée par ce dernier, un champ relatif à l'usage ou aux usages de cette clé U et un champ Plu  
 25 relatif aux plages de validité ou d'utilisation de la clé Kp précitée.

De manière plus particulière, on indique que le champ relatif à l'identifiant de l'utilisateur Uti est rempli par l'utilisateur lors de sa demande de  
 30 certification, alors que les champs relatifs à la valeur de la clé Kp et le champ relatif aux usages de cette clé sont remplis par le système embarqué lui-même.

En ce qui concerne le champ relatif à l'identifiant de l'utilisateur Uti, celui-ci peut correspondre au numéro de série  $SN_i$  du système embarqué lui-même.

5 Une description plus détaillée de la mise en œuvre de l'étape 1012 consistant pour l'autorité de certification à vérifier le message de requête de certification MRCA et en particulier la valeur de contrôle cryptographique  $SC_i$  sera décrite en liaison avec la figure 5.

10 D'une manière générale, on indique que cette étape de vérification est effectuée grâce à un processus de vérification de signature, en particulier de vérification de la valeur de contrôle cryptographique  $SC_i$ , laquelle n'est autre qu'une signature obtenue à partir de la clé privée diversifiée  $KSM_i$  à l'étape 1006 précédemment décrite  
15 dans la description. Dans ces conditions, l'opération de vérification  $\mathcal{V}_{KPM}$  consiste en l'opération duale de celle de celle réalisée à l'étape 1006 précitée.

Ainsi que représenté à la figure 5, les variables d'entrée, outre la clé publique mère  $KPM$  qui a été  
20 retrouvée suite à l'exécution des étapes 1009, 1010 et 1011 des figures 2a ou 2b, sont la valeur de contrôle cryptographique  $SC_i$  et le message de requête de certification MRCA ainsi que l'identifiant  $IDd_i$  du système embarqué, c'est-à-dire l'identifiant de l'opérateur  $OP_i$  et  
25 le numéro de série  $SN_i$  du système embarqué considéré. L'opération de vérification précitée duale de l'opération de signature permet alors, à partir des variables entrées comme paramètres précédemment cités, une réponse par oui ou non, c'est-à-dire l'établissement de la valeur vraie ou de  
30 la valeur complémentée de cette valeur vraie, considérée comme valeur fausse, de l'opération de vérification.

Alors que l'origine de la requête de certification a pu ainsi être vérifiée conformément à la mise en œuvre du

procédé, objet de la présente invention, tel que représenté en figure 2a et/ou 2b, le procédé précité permet également de moduler la puissance des traitements cryptographiques, c'est-à-dire de chiffrement/ déchiffrement et calcul/vérification de signature, alloués à chaque système embarqué Si considéré.

Ainsi, conformément à un aspect particulièrement remarquable du procédé, objet de la présente invention, celui-ci permet, grâce à la certification demandée d'une clé publique donnée et des usages de cette clé publique, soit d'accréditer le système embarqué Si demandeur de cette certification pour réaliser des opérations de déchiffrement selon un processus supporté par un algorithme faible, ou encore de n'accréditer ce système embarqué ou l'entité titulaire de ce système embarqué que pour des opérations supportées par un algorithme limité à des opérations de calcul de signature seulement.

On comprend en particulier qu'en fonction de la valeur des bits de champ d'usage de la clé considérée, valeur d'usage codée par exemple sur 2 bits, la valeur 1X de ces 2 bits pouvant correspondre à un usage de déchiffrement selon un processus supporté par un algorithme faible, et la valeur X1 pouvant correspondre à une opération selon un processus supporté par un algorithme de génération de signature seulement, le système embarqué accrédité pourra réaliser l'une ou l'autre de ces opérations ou bien les deux opérations, mais pas d'autres opérations telles que le déchiffrement fort. Il est aussi précisé qu'un même système embarqué pourra comporter plusieurs clés, certaines comportant par exemple les bits d'usage avec la valeur 10 restreignant ainsi leur usage à des fins de déchiffrement faible et d'autres avec la valeur

01 restreignant ainsi leur usage à des fins de génération de signature.

5 Un processus de déchiffrement supporté par un algorithme faible, conformément à l'objet de la présente invention, sera maintenant décrit en liaison avec la figure 6.

10 De manière générale, on indique qu'une clé de chiffrement ou de déchiffrement utilisée par l'algorithme RSA, clé asymétrique, comprend en général 512 bits ou plus alors qu'une clé symétrique comporte généralement de 40 à 192 bits. Il est donc nécessaire de combler les bits restants, par exemple avec une entête. A titre d'exemple, il est possible, sur la chaîne de 512 bits ainsi créée, de prévoir une en-tête constituée par des valeurs spécifiques  
15 arbitraires fictives, les valeurs 02, 00 et en code hexadécimal FFF suivi de deux octets à la valeur 00 sur toute la valeur de l'en-tête auxquelles est concaténée une clé secrète symétrique, cadrée à droite, l'ensemble constituant une chaîne de bits de 512 bits. Dans le cas où  
20 la clé secrète symétrique KSf comporte 64 bits ou plus, le processus de déchiffrement à clé secrète symétrique est considéré comme fort et ne correspond pas à l'objet de la présente invention dans ce mode de réalisation.

25 Au contraire, lorsque le champ de clé secrète symétrique KSf est inférieur ou égal à 40 bits, le champ d'en-tête étant complété par exemple en conséquence par des valeurs hexadécimales FFF suivie d'un nombre prédéterminé de 00, le champ de clé secrète est un champ de clé secrète de déchiffrement symétrique faible et correspond ainsi à  
30 une fonction de déchiffrement faible susceptible d'être mise en œuvre conformément au procédé objet de la présente invention.

Dans un tel cas et conformément à un aspect particulièrement remarquable du procédé, objet de la présente invention, pour un jeu de clés asymétriques, clé publique de chiffrement notée  $E_p$  et clé privée de 5 déchiffrement  $D_s$  engendrées par le système embarqué  $S_i$ , la clé de chiffrement  $E_p$  correspondant à la clé publique  $K_p$  dont la certification est demandée ainsi que mentionné précédemment dans la description et la clé privée de déchiffrement  $D_s$  correspondant à la clé privée  $K_s$  10 mentionnée précédemment dans la description, le procédé objet de l'invention consiste alors à associer à la clé de déchiffrement  $D_s$  et au processus de déchiffrement asymétrique correspondant, supporté par exemple par l'algorithme RSA, un processus et une clé de déchiffrement 15 faible supporté par exemple par l'algorithme DES et dont la clé symétrique est de longueur inférieure ou égale à 40 bits. Ainsi, en référence à la figure 6, on indique que la clé secrète symétrique faible, notée  $KS_f$ , complétée de son en-tête de valeur arbitraire telle que mentionnée 20 précédemment dans la description, est soumise à un processus de chiffrement pour obtenir une clé chiffrée à partir de la clé publique  $E_p$  de chiffrement asymétrique. La clé chiffrée ainsi obtenue est soumise ensuite à un processus de déchiffrement au moyen de la clé privée de 25 déchiffrement asymétrique  $D_s$  alors que, conformément au procédé objet de la présente invention, cette clé privée de déchiffrement  $D_s$  est mémorisée dans la zone mémoire à accès externe protégé en écriture/lecture du système embarqué et est donc inconnue de l'utilisateur. Le processus de 30 déchiffrement précité permet alors d'obtenir une clé déchiffrée dont la structure n'est autre que l'en-tête précédemment mentionnée dans la description et la clé symétrique faible  $KS_f$  dont la longueur est déterminante.



Si la longueur de la clé symétrique faible KSf est inférieure ou égale à 40 bits, l'en-tête étant simplement discriminée par référence aux valeurs d'en-tête correspondantes et la clé symétrique et en particulier la  
5 clé symétrique faible KSf étant également discriminées en conséquence, cette clé symétrique faible KSf peut alors être mise à disposition de l'entité possédant le système embarqué pour des opérations de déchiffrement selon un processus supporté par un algorithme faible. Dans ces  
10 conditions, la clé symétrique de déchiffrement faible KSf permet à ce dernier de n'assurer que le déchiffrement de cryptogrammes C en messages M au moyen d'un algorithme de déchiffrement faible ainsi que représenté sur la figure 6.

Si au contraire, la longueur de la chaîne de bits  
15 représentative de la clé symétrique autre que l'en-tête précitée est supérieure à 40 bits la clé symétrique, dont la longueur est supérieure à 40 bits, n'est pas mise à disposition de l'entité possédant le système embarqué, laquelle n'est donc pas en mesure d'opérer des opérations  
20 de déchiffrement selon un processus supporté par un algorithme fort.

### REVENDICATIONS

1. Procédé de vérification de l'usage de clés publiques issues d'un jeu de clés asymétriques, clé publique ( $K_p$ ) et clé privée ( $K_s$ ) engendrées, pour un usage  
 5 donné, tel que le chiffrement/déchiffrement ou la vérification/génération de signature numérique, par un système embarqué et mémorisées dans la zone mémoire d'un système embarqué ( $S_i$ ) muni de moyens de calcul cryptographique et de moyens de mémorisation de données  
 10 numériques à accès externe protégé en écriture/lecture, ces données numériques ( $ID_d_i$ ) comportant au moins un numéro de série ( $SN_i$ ) permettant l'identification du système embarqué et un code d'identification ( $OP_j$ ) d'un opérateur habilité à configurer ledit système embarqué et cette requête étant  
 15 formulée par ledit système embarqué par transmission d'un message de requête (MRCA) contenant ladite clé publique ( $K_p$ ) à une autorité de certification (CA), caractérisé en ce que ce procédé consiste :

- préalablement à toute transmission d'une requête  
 20 de certification, lors de la configuration de ces systèmes embarqués par cet opérateur habilité pour tous les systèmes embarqués ( $S_i$ ) d'un ensemble ( $L_k$ ) de systèmes embarqués :
  - à faire engendrer par cet opérateur habilité, pour cet  
 25 ensemble donné de systèmes embarqués, une clé publique mère ( $K_{pM}$ ) et une clé privée mère ( $K_{sM}$ ) mis en œuvre dans le cadre d'un processus supporté par un algorithme ( $CALM$ );
  - à publier ladite clé publique mère ( $K_{pM}$ ) associée à  
 30 l'algorithme ( $CALM$ ), l'identité de cet opérateur habilité ( $OP_j$ ) et à un ensemble ( $L_k$ ) définissant une plage d'identifiants de systèmes embarqués ;
  - à calculer, pour chaque système embarqué appartenant à cet ensemble ( $L_k$ ) de systèmes embarqués, à partir de

ladite clé privée mère ( $K_{SM}$ ) et du numéro de série ( $SN_i$ ) du système embarqué, une clé privée diversifiée ( $K_{SM_i}$ ) et à mémoriser, dans ladite zone mémoire à accès externe protégé en écriture/lecture, ladite clé privée diversifiée ( $K_{SM_i}$ ), et

5       • préalablement à toute transmission d'un message de requête de certification :

- à faire engendrer par l'intermédiaire du système embarqué une requête de certification (RCA), contenant en particulier un champ de la clé publique ( $CAI, K_p$ ) et les indicateurs d'usage (U) de cette clé publique,
- 10       - à calculer, au moyen desdits moyens de calcul et de ladite clé diversifiée ( $K_{SM_i}$ ) associée à ce système embarqué, une valeur de contrôle cryptographique ( $Sc_i$ ) sur l'ensemble de la requête (RCA), ladite valeur de
- 15       contrôle cryptographique étant une signature numérique calculée au moyen de la clé privée diversifiée ( $K_{SM_i}$ );

20       • lors de l'émission, par le système embarqué, d'une requête de certification à l'autorité de certification :

- à former un message de requête de certification (MRCA) contenant la requête (RCA), l'identifiant ( $ID_d$ ) du système embarqué, ce dernier étant constitué d'une part de l'identifiant ( $OP_j$ ) de cet opérateur habilité et d'autre part du numéro de série ( $SN_i$ ) du système
- 25       embarqué, et la valeur de contrôle cryptographique ( $Sc_i$ )
- à transmettre à l'autorité de certification (CA) ledit message de requête (MRCA) formé lors de la phase précédente et contenant la clé publique ( $K_p$ ) et les
- 30       indicateurs d'usage (U), objets de ladite certification, et ladite valeur de contrôle cryptographique ( $Sc_i$ ) ;

      • lors de la réception d'un message de requête de certification (MRCA) par l'autorité de certification :

- à retrouver, l'identité de l'opérateur habilité ( $OP_j$ ) à partir de l'identifiant ( $IDd_i$ ) du système embarqué,
- à retrouver, à partir dudit identifiant ( $OP_j$ ) de cet opérateur habilité la valeur de la clé publique mère ( $KpM$ ) ainsi que l'identifiant de l'algorithme ( $CALM$ ) associé à l'ensemble auquel appartient le système embarqué,
- à vérifier à partir de ladite clé publique mère ( $KpM$ ), dudit numéro de série ( $SN_i$ ) du système embarqué, dudit message de requête de certification reçu ( $MRCA$ ), ladite valeur de contrôle cryptographique ( $Sc_i$ ), ce qui permet d'établir l'authenticité de cette valeur de contrôle cryptographique et l'origine de cette requête de certification.

2. Procédé selon la revendication 1, caractérisé en ce que, lorsque la requête de certification est engendrée par le système embarqué, celui-ci consiste en outre :

- à générer, au niveau du système embarqué, la requête de certification ( $RCA$ ), laquelle est alors composée de trois champs à savoir: un identifiant d'algorithme à clé publique ( $CAL$ ), une valeur de clé publique ( $Kp$ ), et un indicateur des usages de cette clé ( $U$ ).

3. Procédé selon la revendication 1, caractérisé en ce que, lorsque la requête de certification est complétée par le système embarqué lors de l'étape consistant à communiquer audit système embarqué un gabarit de requête de certification ( $GRCA$ ), celui-ci consiste en outre :

- à vérifier, au niveau du système embarqué, la syntaxe du gabarit de requête de certification ( $GRCA$ ) afin de s'assurer qu'il s'agit d'une requête de certification bien formée, et
- à conditionner à une vérification positive, l'étape consistant à faire compléter par le système embarqué les

champs manquants du gabarit de requête de certification (GRCA).

4. Procédé selon la revendication 1, caractérisé en ce que, pour un jeu de clés asymétriques de signature ( $K_p$ ), ( $K_s$ ) engendrées par ledit système embarqué, les moyens de calcul cryptographique de ce système embarqué, n'autorisant d'utiliser la clé privée ( $K_s$ ) qu'à des fins de génération de signature, ladite clé privée ( $K_s$ ) mémorisée dans ladite zone mémoire à accès externe protégé en écriture/lecture étant inconnue de l'utilisateur et restreinte d'utilisation à des fins exclusives de signature numérique, l'utilisation de ladite clé est restreinte à des fins de signature et l'utilisation du certificat contenant la clé publique correspondante est limitée en pratique à des fins de vérification de signature.

5. Procédé selon la revendication 1, caractérisé en ce que, pour un jeu de clés asymétriques clé publique de chiffrement ( $E_p$ ) et clé privée de déchiffrement ( $D_s$ ) engendrées par ledit système embarqué, celui-ci consiste à associer auxdites clés ( $E_p$ ), ( $D_s$ ) et processus de déchiffrement asymétrique un processus et une clé de déchiffrement symétrique "faible", la clé symétrique de déchiffrement étant chiffrée puis déchiffrée au moyen de la clé privée de déchiffrement asymétrique ( $D_s$ ), ladite clé privée ( $D_s$ ) mémorisée dans ladite zone mémoire à accès externe protégé en écriture/lecture étant inconnue de l'utilisateur, ce qui permet de n'autoriser l'utilisation de ladite clé qu'à des fins de déchiffrement faible et l'utilisation du certificat contenant la clé publique correspondante étant limitée en pratique à des fins de chiffrement faible.

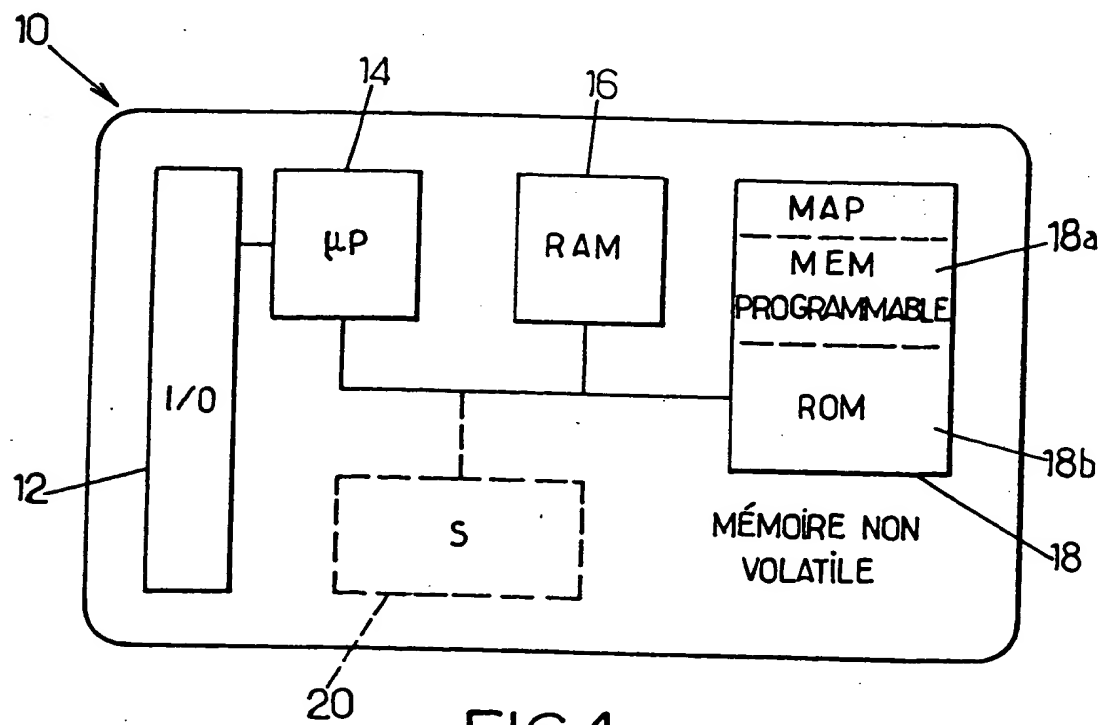


FIG.1.  
(ART ANTÉRIEUR)

FIG.2a.

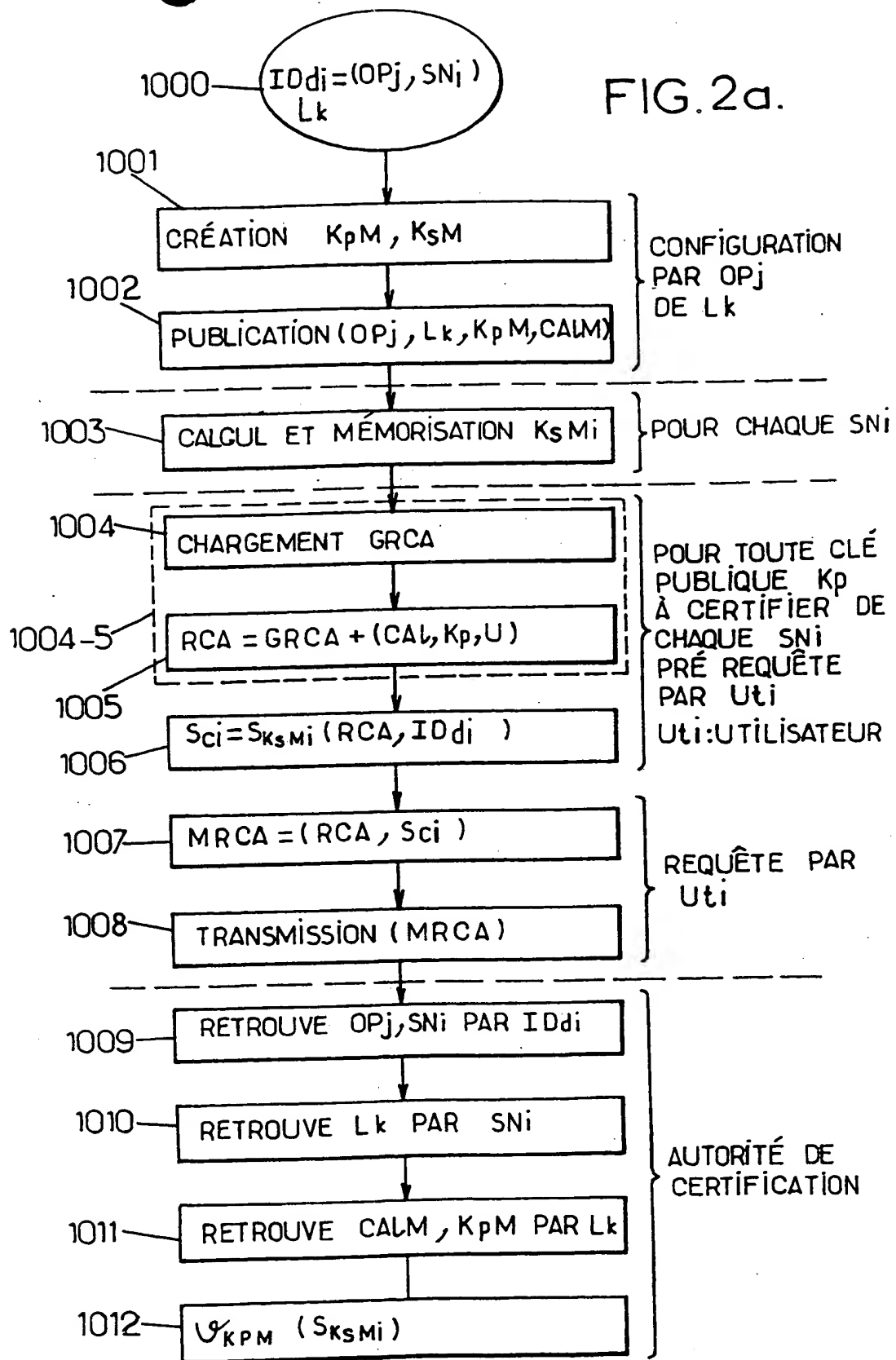


FIG.2b.

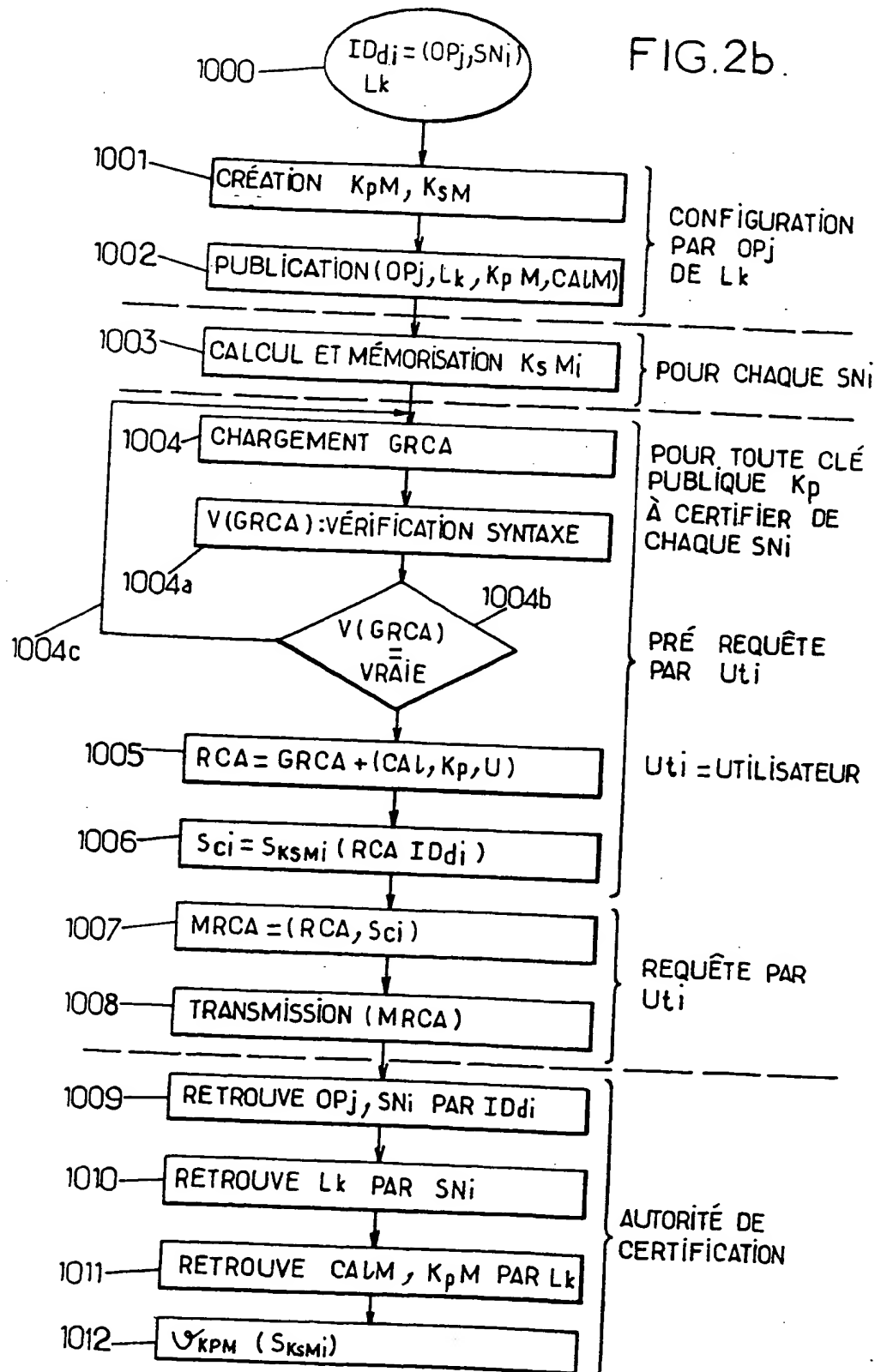




FIG.3.

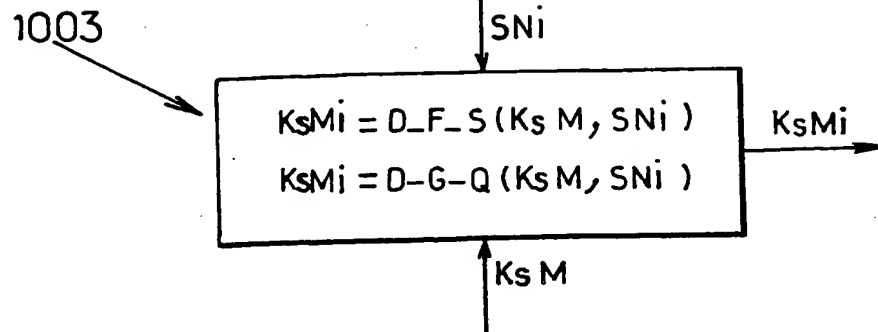


FIG.5.

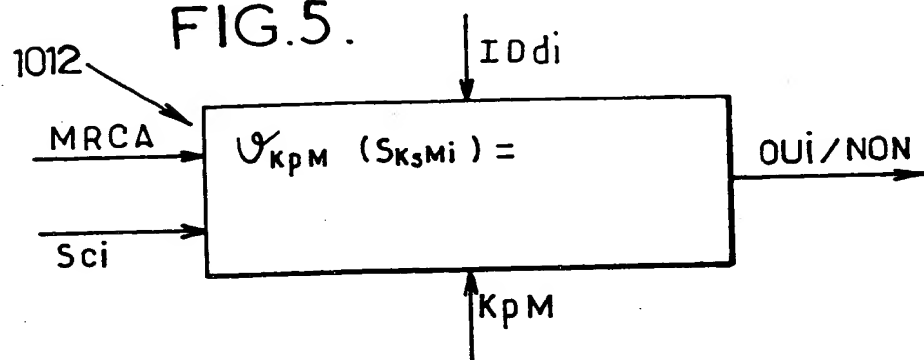


FIG.6.

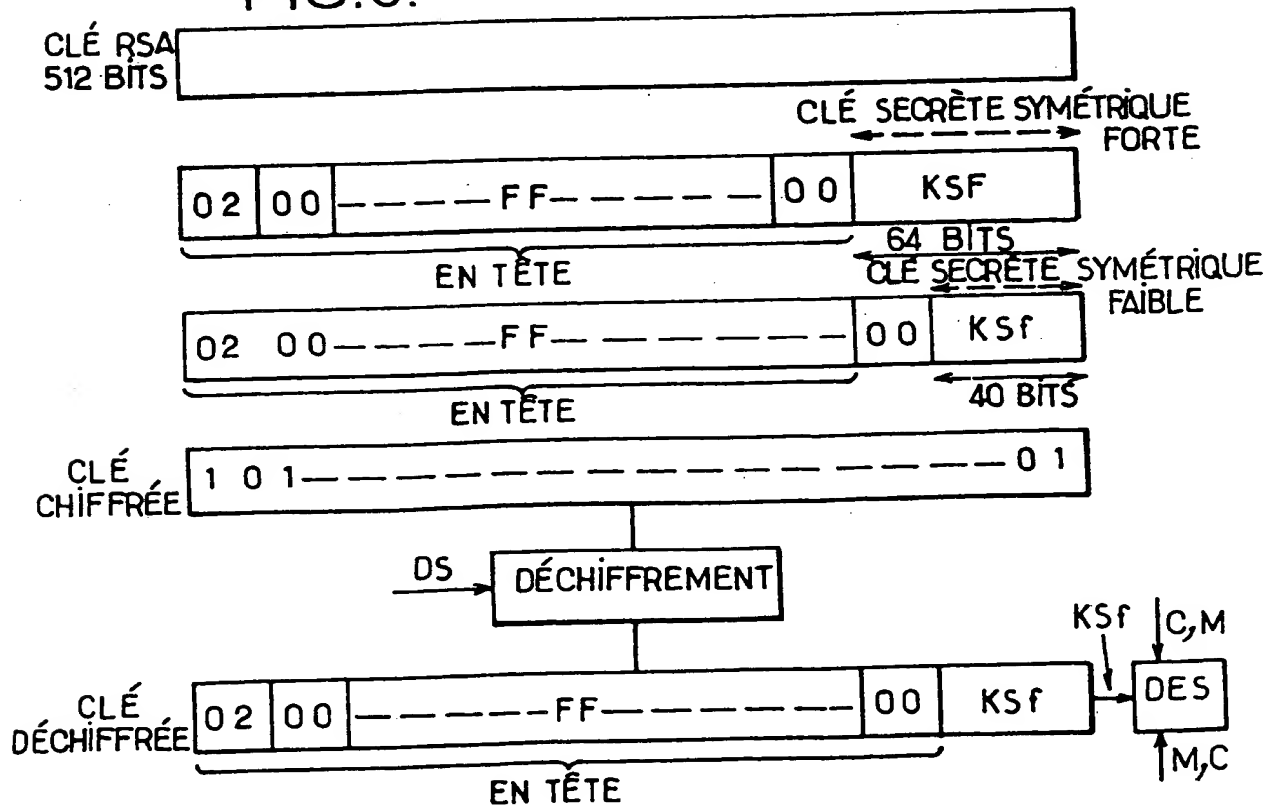


FIG.4a.

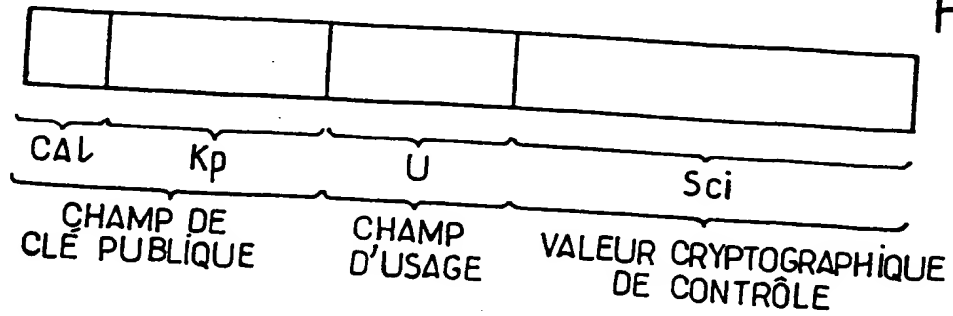
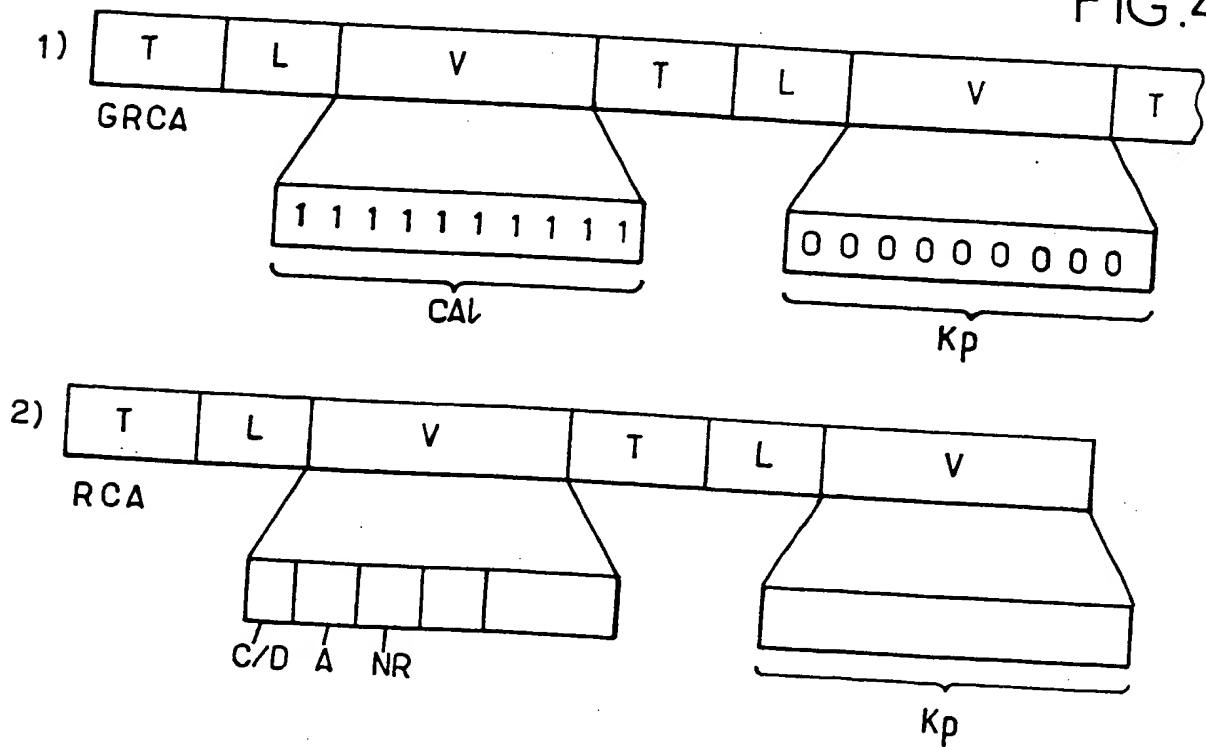
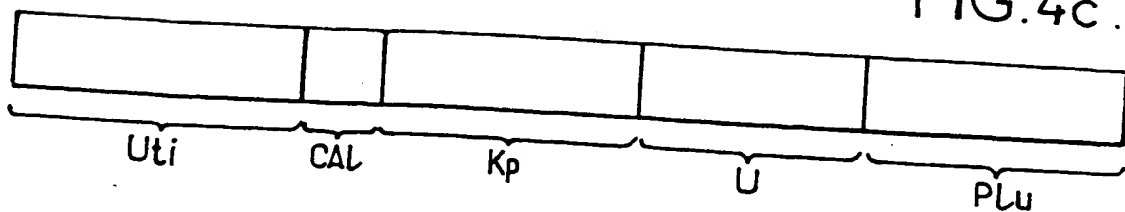


FIG.4b.



GRCA

FIG.4c.



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

---

**THIS PAGE BLANK (USPTO)**